Quality *Integrity* *Accountability*

DoD IG Report to Congress on Section 357 of the National Defense Authorization Act for Fiscal Year 2008

Review of Physical Security of DoD Installations

Report No. D-2009-035

(Project No. D2008-D000LB-0159.000)

January 14, 2009

Special Notice

This document contains information provided as a nonaudit service. Therefore, any work performed was not done in accordance with Generally Accepted Government Auditing Standards.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
14 JAN 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Review of Physical Security of DoD Installations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense Inspector General,ODIG-AUD,400 Army Navy Drive,Arlington,VA,22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**18**	

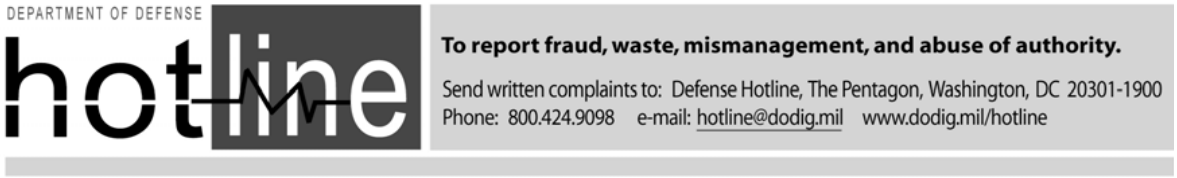
Additional Information and Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest ideas for or to request future audits, contact the Office of the Deputy Inspector General for Auditing at (703) 604-9142 (DSN 664-9142) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704



Acronyms and Abbreviations

ASD[NII]/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
DBIDS	Defense Biometric Identification System
DEERS	Defense Enrollment Eligibility Reporting System
DMDC	Defense Manpower Data Center
DTM	Directive-Type Memorandum
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standard
GAO	Government Accountability Office
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive-12
NACI	National Agency Check With Inquiries
NDAA	National Defense Authorization Act
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PACS	Physical Access Control System
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

Background

Section 357 of Public Law 110-181, "National Defense Authorization Act for Fiscal Year 2008," January 28, 2008 (NDAA 2008), requires the DoD Office of Inspector General (DoD IG) to submit to Congress a report on the physical security of DoD installations and resources. The report, due January 27, 2009, is to include:

- an analysis of the progress in implementing requirements under the Physical Security Program as set forth in the DoD Regulation 5200.08–R, Chapter 2 (C.2), "Policy Objectives," and Chapter 3 (C3.3), "Installation Access," which mandate the policies and minimum standards for the physical security of DoD installations and resources;

- recommendations based on the findings of the Government Accountability Office (GAO) in Report No. GAO-08-120SU, **"**MILITARY BASES: High-Level Access Control Guidance Is Consistent, but Flexible For Local Circumstances and Evolving to Standardize Access Controls," October 12, 2007. This report was required by section 344 of the "John Warner National Defense Authorization Act for Fiscal Year 2007" (NDAA 2007, P.L. 109–366; 120 Stat. 2155); and

- recommendations based on the lessons learned from the thwarted plot to attack Fort Dix, New Jersey, in 2007.

Scope and Methodology

DoD IG officials met with staff from the House Armed Services Committee on February 14, 2008, and a member of Representative Norman Dicks' staff on March 3, 2008. DoD IG officials agreed to provide a review of physical security at DoD installations based on an ongoing audit of DoD implementation of Homeland Security Presidential Directive-12 (HSPD-12). We agreed that this review would be done as a nonaudit service because it is based on audit work performed for the HSPD-12 audit. We issued our HSPD-12 report, No. D-2008-104, on June 23, 2008. In addition, congressional staff requested that we provide information on contract guard services provided on DoD military installations. Finally, we list DoD groups formed to assist with the DoD Physical Security Program and recommendations from our HSPD-12 report.

Summary

The findings and recommendations for "DoD Implementation of Homeland Security Presidential Directive-12," Report No. D-2008-104, June 23, 2008, served as the basis for this review. Both the DoD IG audit and congressionally mandated actions have resulted in DoD's reexamining and revising its physical security policy. DoD personnel responsible for implementing the HSPD-12 recommendations have already begun reporting progress and actions taken. We will review the reported actions during the HSPD-12 report follow-up and mediation process.

The Under Secretary of Defense (Intelligence) Directive-Type Memorandum (DTM) 08-004, "Policy Guidance for DoD Access Control," April 29, 2008 (see Appendix A), and a revised DoD Regulation 5200.08-R, "Physical Security Program," chapter 3, April 9, 2007, further clarified the existing guidance for upgrading access control systems. DoD intends to make additional substantial revisions to DoD Regulation 5200.08-R by February 2009.

The Office of Management and Budget (OMB) issued "Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation," May 23, 2008, to assist Federal agencies in preparing or refining plans for incorporating the use of Personal Identity Verification (PIV) credentials with physical and logical access control systems.

DoD's Physical Security Program is a work-in-progress. The GAO October 2007 report found that the Office of the Secretary of Defense had issued broad, overarching, access control-related guidance, but provided commanders with flexibility to tailor security measures to the specific needs of their installations. This flexibility leads to a lack of consistency, which directly relates to the differences GAO found in the access control procedures at the 12 installations it reviewed (8 within and 4 outside the United States). The GAO report identified eight U.S. installations as having access control procedure deficiencies. In telephone interviews with us, installation physical control personnel from the eight installations stated that they had not completed any updates to access control procedures. We are not making any recommendations because of the ongoing updates DoD is making to its physical access control policy, as required by NDAA 2008, Section 1069. (See Appendix B.)

The lessons learned from the Fort Dix plot disclosed how terrorists targeted installations with low physical security and how critical it is to protect DoD personnel by implementing a solid Physical Security Program. HSPD-12 directed Federal agencies to implement a Government-wide standard for secure and reliable forms of identification that are strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation and can be rapidly authenticated electronically. However, DoD's full implementation of HSPD-12 will not be completed until some time after summer 2012. We believe that full implementation of HSPD-12 and the policy changes USD(I) is making as required by NDAA 2008, Section 1069, will address threats to DoD installations like the one at Fort Dix. Therefore, we are not making any recommendation.

The recommendations in our HSPD-12 report, GAO report, and the lessons learned from the plot at Fort Dix address multiple issues with the DoD Physical Security Program. USD(I)'s current efforts to establish a baseline standard for access controls will decrease the likelihood of inconsistent implementation of access-control procedures across DoD installations and components and strengthen the DoD Physical Security Program.

Table of Contents

FY 2008 National Defense Authorization Act

SEC. 357. DEPARTMENT OF DEFENSE INSPECTOR GENERAL REPORT ON PHYSICAL SECURITY OF DEPARTMENT OF DEFENSE INSTALLATIONS.

(a) REPORT.—Not later than one year after the date of the enactment of this Act, the Inspector General of the Department of Defense shall submit to Congress a report on the physical security of Department of Defense installations and resources.

(b) ELEMENTS.—The report required by subsection (a) shall include the following:

(1) An analysis of the progress in implementing requirements under the Physical Security Program as set forth in the Department of Defense Instruction 5200.08–R, Chapter 2 (C.2) and Chapter 3, Section 3: Installation Access (C3.3), which mandates the policies and minimum standards for the physical security of Department of Defense installations and resources.

(2) Recommendations based on the findings of the Comptroller General of the United States in the report required by section 344 of the John Warner National Defense Authorization Act for Fiscal Year 2007 (Public Law 109–366; 120 Stat. 2155).

(3) Recommendations based on the lessons learned from the thwarted plot to attack Fort Dix, New Jersey, in 2007.

Progress in Implementing Requirements for DoD Regulation 5200.08-R Chapters 2 and 3 (C3.3)

DoD Regulation 5200.08-R, Chapter 2

Chapter 2, "Policy Objectives," defines physical security program as the part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, and information and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. Chapter 2 requires the use of biometric, electronic, or mechanical technological security systems to both mitigate vulnerability to the threat and reduce reliance on fixed security forces and mandates compliance with Federal Information Processing Standards (FIPS) 201-1[1] guidance for the acquisition of Federal PIV credentials and supporting access control equipment.

HSPD-12 Report Results

To identify the DoD's progress in implementing Physical Security in Chapter 2, "Policy Objectives," we used the results of our audit Report No. D-2008-104, "DoD Implementation of Homeland Security Presidential Directive-12," June 23, 2008, which we conducted from March 2007 through February 2008. The report identified deficiencies in the implementation of the requirements of Chapter 2. Specifically, DoD installations did not include the use of biometric, electronic and/or mechanical technological security systems to both mitigate vulnerability to the threat and reduce reliance on fixed security forces in their physical security planning. DoD did not comply with the requirements for the development of the FIPS 201-1 identity authentication. DoD Components were purchasing noncompliant HSPD-12 access control equipment, which is contrary to Chapter 2. Components cited the conflicting guidance in DoD Regulation 5200.08-R as reasons for their continued acquisition of the Defense Biometrics Identification System (DBIDS), which is noncompliant with HSPD-12 requirements.

Our report recommended that the Under Secretary of Defense for Intelligence (USD[I]) revise DoD Instruction 5200.08, "Security of DoD Installations and Resources," and DoD Regulation 5200.08-R, "Physical Security Program," to appropriately reflect responsibility for incorporating FIPS 201-1 minimum requirements in all DoD access control systems. USD(I) agreed to revise the guidance to require all electronic access control systems to meet HSPD-12 and OMB guidance and to remove conflicting references for access control systems policy. USD(I) agreed to coordinate with Under Secretary of Defense for Acquisition, Technology, and Logistics to perform research, development, test, and evaluation of all procurements for electronic access control systems in coordination with the Components' physical security representatives and electronic systems engineers. As a result, USD(I) issued DTM 08-004, "Policy Guidance for DoD Access Control," April 29, 2008,

[1] FIPS Publication 201-1, "Personal Identity Verification (PIV) for Federal Employees and Contractors," March 2006, as directed by HSPD-12, establishes the standard that specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems.

which requires USD(I) to identify capabilities, requirements, and baseline standards for a comprehensive suite of hardware and software solutions to provide Components with the necessary tools to verify and authenticate the identities of personnel entering their facilities and manage the physical access authorizations or denials. The DTM requires DoD Component heads to ensure that when purchasing upgrades to existing access control systems or replacing current systems, the upgrades meet FIPS 201-1.

DoD Regulation 5200.08-R, Chapter 3, Section C3.3

Chapter 3, "Installation Access and Emergency Planning," implements general procedures that meet minimum Federal standards for controlling entry and exit at military installations and facilities within those installations. Specifically, Section C3.3, "Installation Access," states that HSPD-12 mandates policy for a common identification standard for all Federal employees and contractors and that agencies are to develop and implement a mandatory standard for secure and reliable forms of identification. Section C3.3 states that a National Agency Check With Inquiries (NACI) is required for permanent issuance of the credential, and credentials issued to individuals without a completed NACI must be electronically distinguishable. Also, Section C3.3 requires that the installations and facilities continue using a locally established, temporary issue, visitor identification system for occasional visitors. Section C3.3 requires that the DBIDS card be issued and authorized for routine physical access to a single DoD installation or facility. Further, upon full implementation of the Common Access Card, which is the standard DoD PIV access control credential, and the DBIDS credential, all other non-FIPS 201-1 compliant badges and associated equipment used for physical access are to be eliminated.

HSPD-12 Report Results

To identify the progress in implementing the requirements of DoD 5200.08-R, Chapter 3 (C3.3), "Installation Access," we analyzed it in relation to the results of our HSPD-12 audit. Our June 2008 report showed that DoD did not meet the requirements of Chapter 3 (C3.3). Further, Chapter 3 did not properly reflect HSPD-12/FIPS 201-1 requirements as it advocated the use of a noncompliant physical access system. Thus, DoD had not developed and issued comprehensive HSPD-12 implementation guidance to DoD Components. The DoD installations we visited during our audit expressed uncertainty about how to proceed with implementation of HSPD-12 as no overall DoD guidance had been issued. As a result, DoD Components were delaying their preparations for HSPD-12.

In our HSPD-12 report, we recommended that the Under Secretary of Defense for Personnel and Readiness (USD[P&R]) develop and issue a directive to achieve full DoD compliance with the requirements of HSPD-12. USD(P&R) agreed with our recommendation. We also recommended that USD(I) delete the DBIDS language in paragraph C3.3.2 in its entirety and the reference to the DBIDS credential in paragraph C3.3.3 of the Installation Access section. USD(I) agreed and issued DTM 08-004, April 29, 2008, deleting paragraph C3.3.2., in its entirety, and the DBIDS reference in paragraph C3.3.3 from DoD 5200.08-R.

Additionally, OMB issued "Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation," May 23, 2008, to assist agencies with their implementation activities for HSPD-12. One of the recommended steps in the OMB guidance is for the agencies to perform a full inventory of their physical access control systems, including card readers, which would help the agencies in determining what they have and what they need to complete PIV credentials for physical access control.

DoD's PIV credential remains in a transitional state and is projected to meet FIPS 201-1 end-point compliance in summer 2012, missing the original milestone of April 2010. Our audit found that DoD had not completed work on developing the mandatory public key infrastructure (PKI) authentication certificate and PIV applet necessary for a secure, reliable and interoperable credential. As a result, we recommended that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD[NII]/DoD CIO) develop the mandatory PKI authentication certificate that complies with FIPS 201-1 requirements. ASD(NII)/DoD CIO disagreed with our recommendation, citing extenuating circumstances that would not allow it to comply. The matter is under mediation. We also recommended that USD(P&R) submit DoD's proposed PIV end-point credential to the General Services Administration (GSA) for conformance and interoperability testing. USD(P&R) agreed with our recommendation, stating that it would submit its Common Access Card PIV end-point credential to GSA for conformance and interoperability testing within 1 month of completing the PKI authentication certificate.

DoD and other Federal agencies did not meet the deadline set by OMB for completing background checks for all current employees and contractors employed for fewer than 15 years. DoD has yet to establish the required electronic indicator to verify that all individuals receiving the PIV credential have at least initiated, if not completed, the required NACI-equivalent background checks. DoD does not intend to produce identity credentials that include the required electronic indication of the status of a NACI-equivalent. In our report, we recommended that USD(P&R) issue a directive assigning clear responsibility for compliance with each aspect of HSPD-12, including background check requirements. USD(P&R) agreed with the recommendation. We also recommended that USD(I) revise DoD Regulation 5200.08-R to require all contractors and Federal employees needing routine physical access to a DoD installation to undergo a NACI-equivalent background investigation and then be issued a DoD PIV credential. USD(I) agreed with the recommendation.

Government Accountability Office Report 08-120SU, October 2007

On October 17, 2006, Congress passed the "John Warner National Defense Authorization Act of 2007," which in section 344 required GAO to assess the extent to which each DoD installation has or would benefit from having an access control system with the ability to:

1. electronically check any Federal, State, or local Government identification card;
2. verify that an identification card used to obtain access to the installation was legitimately issued and not reported lost or stolen;
3. check on a real-time basis all relevant watch lists maintained by the Government, including terrorist watch lists and lists of persons wanted by Federal, State, or local law enforcement authorities;
4. maintain a log of individuals seeking access to the installation and individuals who are denied access; and
5. exchange information with any installation having a system that complies with the standards and protocols.

GAO Findings

GAO reviewed access control guidance for 12 DoD installations (8 in the United States and 4 outside), Service-level access control procedures, and three pilot access control systems. The GAO objectives and findings were as follows.

(1) Identify the extent to which consistency exists in standards, protocols, and procedures for access control, and the extent to which this guidance addresses the five capabilities listed in the mandate (NDAA 2007). The report stated that the Office of the Secretary of Defense had issued broad, overarching, access control-related guidance, but provided flexibility to commanders to tailor security measures to specific needs of their installation, which diminishes DoD-wide consistency.

(2) Identify the extent to which the establishment of joint standards and protocols for access controls at installations has addressed or would address force protection needs both generally and as they relate to the five capabilities listed in NDAA 2007. GAO found that 9 of the 12 DoD installations addressed two or fewer of the five capabilities in their written procedures; three installations did not address any of the capabilities.

The GAO report was based and performed under the requirements of the "John Warner National Defense Authorization Act for Fiscal Year 2007," Section 344, "Comptroller General Report on joint standards and protocols for access control systems at Department of Defense installations." NDAA 2007, section 344 did not require GAO to provide report recommendations, and GAO did not make any recommendations.

DoD IG Results

As stated in our June 2008 report, USD(I) is revising DoD Regulation 5200.08-R to meet the requirements of NDAA 2008, section 1069. Section 1069 requires the Secretary of Defense to develop access standards applicable to all military installations of the United States. The standards are to include protocols to determine the fitness of an individual to enter an installation and standards and methods for verifying the identity of the individual. These requirements incorporate the five capabilities addressed in the GAO Report and found in DoD Regulation 5200.08-R. Section 1069 set the following deadlines:

- Develop standards required by not later than July 1, 2008;[2]
- Implement standards by not later than January 1, 2009; and
- Submit standards to Congress not later than August 1, 2009.

We are not making any recommendations because DoD's planned revisions will address the deficiencies cited in the GAO report.

Lessons Learned From the Fort Dix Plot

Background

From January 3, 2006, to May 7, 2007, six individuals, later known as the Fort Dix Six, prepared for an attack on soldiers at Fort Dix, New Jersey. They selected Fort Dix after researching nine potential targets in the United States. The group's actions included recruiting members, obtaining firearms, surveying potential targets, selecting a target, obtaining a map of the selected target area, and conducting firearms training. The Federal Bureau of Investigation (FBI) placed the group under surveillance as a result of a tip from an electronic store clerk that received a videotape from one of the members of the Fort Dix Six, who brought it to the store to be duplicated. The tape showed 10 young men shooting assault weapons at a firing range, calling for jihad (a Muslim holy war), and shouting "Allah Akbar" (God is great). During the surveillance, two informants infiltrated the group and obtained intelligence on the group's actions. The FBI was able to prevent the attack on Fort Dix as a result of the intelligence obtained by the informants.

Results

We obtained the lessons learned from the Fort Dix plot from the Defense Criminal Investigative Service. The lessons learned disclosed the targeting of bases that displayed low physical security and the avoidance of bases that displayed high physical security. This shows the important role physical security plays in antiterrorism and force protection. It illustrates how critical physical security measures are in protecting DoD personnel. Random antiterrorism measures play a key role in determining

[2] USD(I) submitted a petition to Congress to revise the July 1, 2008 due date to develop standards by February 1, 2009, and fully implemented by February 1, 2012.

targeting by making base security less predictable. Also, critical infrastructure protection of information systems is important because the destruction of critical infrastructure hardware can lead to complete mission failure or an exploitable vulnerability during a terrorist attack.

HSPD-12

The use of multiple identity credentials poses an increased terrorist threat to U.S. Federal facilities. The President recognized the need to increase the protection of U.S. Federal facilities and signed HSPD-12 on August 27, 2004. HSPD-12 policy requires the development of a mandatory Government-wide standard for a common secure and reliable form of identification issued by the Federal Government to its employees and contractors that is strongly resistant to terrorist exploitation and enhances security. In our Report No. D-2008-104, we reported that DoD has missed key milestones for implementing HSPD-12 standards for a common identification card used for access to Federal facilities and information systems. We concluded that DoD's inconsistent approaches to the security of facilities and information systems are inefficient and costly, and they increase risk to the DoD facilities. We recommended that DoD take the necessary action to issue comprehensive HSPD-12 implementing guidance DoD-wide and produce the mandatory HSPD-12 credential. DoD is implementing the lessons learned from the Fort Dix plot and is revising its Physical Security policy as it addresses the recommendations we made in our HSPD-12, June 2008 report. Therefore, we are not making any additional recommendations.

Ongoing and Prior Audit Coverage of Contract Guards

DoD IG officials spoke with a staff member of the House Armed Services Committee on March 3, 2008, to clarify the NDAA 2008 mandate and provide assurance that we would address congressional concerns in our review. Also, we agreed to identify the status of work performed on contract guard services.

We identified one ongoing and two prior audit reports on contract guard services.

Representative Christopher H. Smith requested that DoD IG review the security guard services contract at Naval Weapons Station Earle, New Jersey (Project No. D2008-D000CG-0116). The audit objective was to determine whether the Navy properly administered the security guard services contract and whether the contractor performed according to contract requirements. The final report for that audit is scheduled for release in January 2009.

We identified two prior audit reports, GAO-06-284, "Army's Guard Program Requires Greater Oversight and Reassessment of Acquisition Approach," April 2006, and Army Audit Agency, A-2008-0017-ALE, "Administration for Guard Services Contracts in Europe," November 8, 2007. The GAO report focused on the Army's acquisition approach; the effectiveness and adequacy of the security guard screening process; the adequacy of security guard training; and the rationale for and implementation of award fees. The Army Audit Agency determined that the Army may have hired and retained security guards who did not meet the qualifications and training requirements specified in the contract.

Multiple Groups Working on DoD Physical Security

Multiple DoD groups have been formed to assist with the DoD Physical Security Program and HSPD-12 implementation. The groups stated objectives include: development of Physical Security guidance and policy; designing and acquiring more efficient security equipment; integrating, and synchronizing biometric technologies; and setting strategy and providing oversight. The groups are listed as follows:

1. Physical Security Review Board
2. Physical Security Equipment Action Group
    a. Security Equipment Integration Working Group
    b. Joint Requirements Working Group

Biometrics Task Force[3]
Identity Protection and Management Senior Coordinating Group[3]

Recommendations for DoD's HSPD-12 Program

The recommendations we made in our Report No. D-2008-104, "Implementation of Homeland Security Presidential Directive-12," June 23, 2008, that apply to this review are listed below and are referenced throughout this report. They include the following.

A.1. We recommend that the Under Secretary of Defense for Personnel and Readiness:

a. Submit DoD's proposed personal identity verification end-point credential to the General Services Administration for conformance testing and approval within 1 month of completion of Recommendation A.3.

A.3. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer develop the mandatory Public Key Infrastructure authentication certificate that complies with FIPS 201-1 requirements to use Common Policy object identifiers for cross-agency verification of cardholders' identification within 6 months.

B.1. We recommend that the Under Secretary of Defense for Personnel and Readiness develop and issue within 3 months a Deputy Secretary of Defense Directive to achieve full Department of Defense compliance with the requirements of Homeland Security Presidential Directive-12. The Directive should assign clear responsibility for compliance with each aspect of HSPD-12 and specify milestones for achieving compliance.

[3] These working groups support Physical Security efforts.

B.2. We recommend that, within 3 months, the Under Secretary of Defense for Personnel and Readiness and the Under Secretary of Defense for Intelligence:

a. Revise DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program," DoD Instruction 5200.08, "Security of DoD Installations and Resources," DoD Regulation 5200.08-R, "Physical Security Program," and other DoD issuances as necessary to appropriately reflect responsibility for incorporating FIPS 201-1 minimum requirements in all DoD electronic access control systems.

b. Develop minimum background check requirements for vetting foreign nationals in countries where no international security agreement exists, such as Iraq and Afghanistan.

B.3. We recommend that the Under Secretary of Defense for Intelligence:

a. Revise DoD Regulation 5200.08-R, "Physical Security Program," April 9, 2007, within 3 months to:

(1) Require all contractors and Federal employees requiring routine physical access to a DoD installation to undergo a NACI background investigation and receive a DoD PIV credential.

(3) Delete paragraph C3.3.2 in its entirety and delete the reference to the Defense Biometric Identification System credential in paragraph C3.3.3 of the Installation Access section.

Appendix A. Under Secretary of Defense (Intelligence) Directive-Type Memorandum 08-004 "Policy Guidance for DoD Access Control"

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

APR 29 2008

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 08-004, "Policy Guidance for DoD Access Control"

References: (a) DoD 5200.08-R, "Physical Security Program," April 9, 2007
(b) Homeland Security Presidential Directive (HSPD)-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
(c) Federal Information Processing Standard (FIPS) 201, March 2006

Purpose. This DTM clarifies guidance for physical access equipment. This DTM is effective immediately; it shall be incorporated into DoD 5200.08-R within 180 days.

DoD 5200.08-R implements the requirements of Reference (b) for physical access. In complying with HSPD-12, the Department of Defense will develop a robust interoperable system that raises security standards.

HSPD-12 requires establishment of a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees) to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Reference c is the approved Government-wide standard. DoD 5200.08-R allows for legacy access control systems to be used during the HSPD-12 transition. These systems require interfacing hardware using commercial off-the-shelf solutions to complete the access control system. We are engaging the physical security community and industry to assess the availability of access control capabilities that are FIPS 201 compliant.

Upon completion of this assessment, we will provide further guidance. Changes will be incorporated in DoD 5200.08-R during periodic updates. Any questions or concerns regarding access control policy may be requested from my office. My point of contact is Donna Rivera at donna.rivera@osd.mil or (703) 604-1172.

Applicability. This DTM applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (referred to collectively as the "DoD Components").

Responsibilities.

- The Under Secretary of Defense for Intelligence shall identify capabilities, requirements, and baseline standards for a comprehensive suite of hardware and software solutions to provide Components the necessary tools to verify and authenticate the identities and manage physical access authorizations or denials for personnel entering their facilities.

- The Heads of the DoD Components shall apply the following interim guidance when replacing electronic access control equipment until final guidance is issued: when purchasing upgrades to existing access control systems or when replacing current systems, the upgraded system must meet FIPS 201 (including ISO 14443 contactless technology and ability to perform automated personal identity verification); include an emergency power source; and have the ability to provide rapid electronic authentication to Federal and DoD authoritative databases, including DoD personnel registered in the Defense Enrollment and Eligibility Reporting System.

Procedures.

Change the first sentence of paragraph C1.3.4 of DoDD 5200.08-R to read "Standardize personal identification and authentication to DoD installations and facilities, including interoperability with other Federal entities, utilizing the DoD PIV credential (Common Access Card (CAC)) as the universal authority of individual authenticity, consistent with applicable law."

Change the fourth sentence of paragraph C3.3.1 of DoDD 5200.08-R to read "Consistent with applicable law, the CAC shall be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces."

Change DoD 5200.08-R to delete paragraph C3.3.2. in its entirety on page 17 and delete the first sentence of paragraph C3.3.3.on page 18 "Upon full implementation of the CAC, the standard DoD PIV access control credential and the DBIDS credential, eliminate all other non-FIPS 201 compliant badges and associated equipment used for physical access (see Reference (r))."

Releasability. UNLIMITED. This DTM is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

James R. Clapper, Jr.

Appendix B. National Defense Authorization Act for Fiscal Year 2008, Section 1069

PUBLIC LAW 110–181—JAN. 28, 2008 122 STAT. 326

SEC. 1069. STANDARDS REQUIRED FOR ENTRY TO MILITARY INSTALLATIONS IN UNITED STATES.

(a) DEVELOPMENT OF STANDARDS.—

(1) ACCESS STANDARDS FOR VISITORS.—The Secretary of Defense shall develop access standards applicable to all military installations in the United States. The standards shall require screening standards appropriate to the type of installation involved, the security level, category of individuals authorized to visit the installation, and level of access to be granted, including—

(A) protocols to determine the fitness of the individual to enter an installation; and

(B) standards and methods for verifying the identity of the individual.

(2) ADDITIONAL CRITERIA.—The standards required under paragraph (1) may—

(A) provide for expedited access to a military installation for Department of Defense personnel and employees and family members of personnel who reside on the installation;

(B) provide for closer scrutiny of categories of individuals determined by the Secretary of Defense to pose a higher potential security risk; and

(C) in the case of an installation that the Secretary determines contains particularly sensitive facilities, provide additional screening requirements, as well as physical and other security measures for the installation.

(b) USE OF TECHNOLOGY.—The Secretary of Defense is encouraged to procure and field existing identification screening technology and to develop additional technology only to the extent necessary to assist commanders of military installations in implementing the standards developed under this section at points of entry for such installations.

(c) DEADLINES.—

(1) DEVELOPMENT AND IMPLEMENTATION.—The Secretary of Defense shall develop the standards required under this section by not later than July 1, 2008, and implement such standards by not later than January 1, 2009.

(2) SUBMISSION TO CONGRESS.—Not later than August 1, 2009, the Secretary shall submit to the Committees on Armed Services of the Senate and House of Representatives the standards implemented pursuant to paragraph (1).